Today we will be doing a walkthrough on BrainFuck. So lets get going.

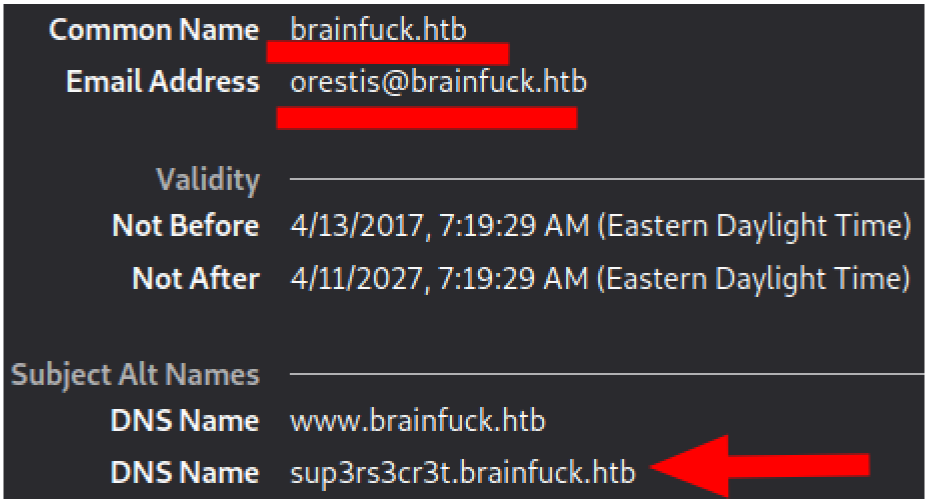
Enumeration:

```
Starting Nmap 7.91 ( https://nmap.org ) at 2021-10-24 14:16 EDT
Nmap scan report for 10.129.244.189
Host is up (0.040s latency).
Not shown: 995 filtered ports
PORT    STATE SERVICE
22/tcp  open  ssh
25/tcp  open  smtp
110/tcp open  pop3
143/tcp open  imap
443/tcp open  https

Nmap done: 1 IP address (1 host up) scanned in 10.18 seconds
```

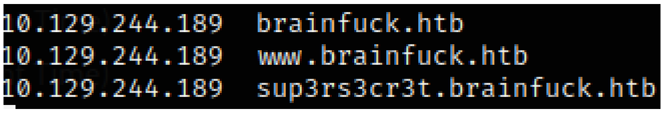
There are three mail ports open hinting towards possibly there is some sensitive information present in the mailbox. But to access we need email address and a password which we neither have. We can brute force ssh but that would be waste of time too. So our focus should be port 443 or the webserver.

Port 443

If you just paste the IP address, it will show you "Welcome to nginx" page which you normally get after first time installation. For this to work properly we need virtual host. If you review the certificate which is presented when navigating to this address, 2 juicy information is disclosed. Two virtual hosts which we need to add in our hosts file and an email address.

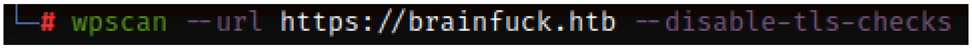


```
Common Name      brainfuck.htb
Email Address    orestis@brainfuck.htb

Validity
Not Before       4/13/2017, 7:19:29 AM (Eastern Daylight Time)
Not After        4/11/2027, 7:19:29 AM (Eastern Daylight Time)

Subject Alt Names
DNS Name         www.brainfuck.htb
DNS Name         sup3rs3cr3t.brainfuck.htb
```



```
10.129.244.189  brainfuck.htb
10.129.244.189  www.brainfuck.htb
10.129.244.189  sup3rs3cr3t.brainfuck.htb
```

The home page contains a comment from admin that SMTP congifuration is ready and email address is present which we found earlier from the certificate. If you navigate through the site there is nothing more interesting except that it is running wordpress 4.7.3 (from Wappalyzer extension) and a comment which says the user's dog name is jack which can be included in the password wordlist. I reckon its already present in rocky you. Lol never mind. We can try to brute force the wpadmin login page but lets keep that for last resort. Lets run wpscan if we can find any vulnerable plugins or themes. Make sure to disable tls checks while running wpscan.



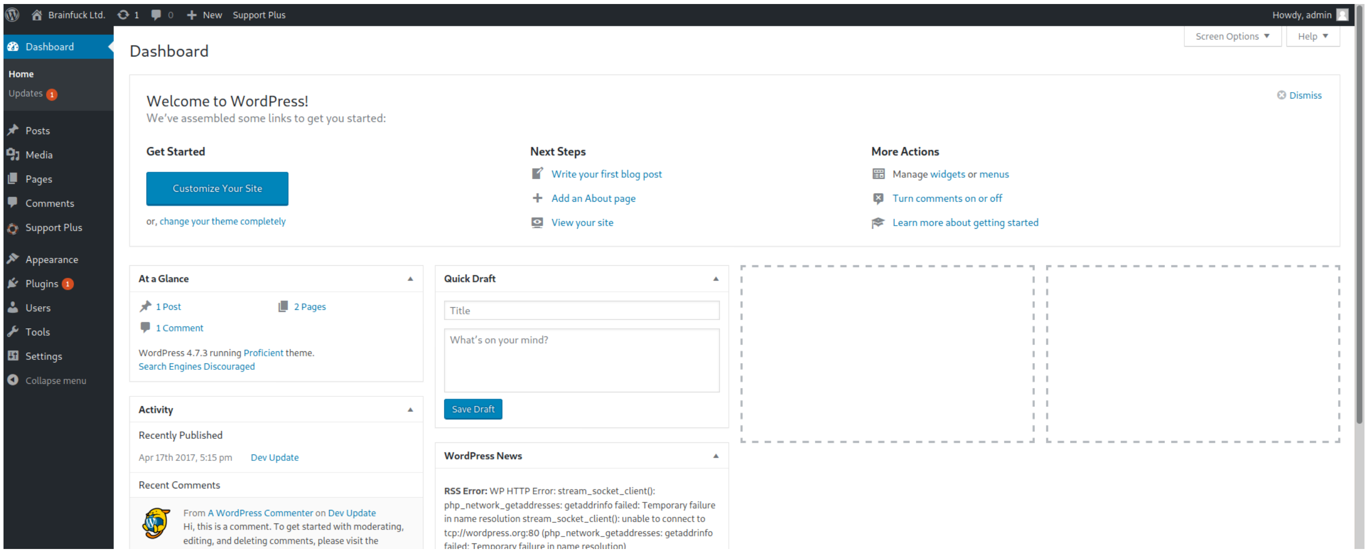
```
└─# wpscan --url https://brainfuck.htb --disable-tls-checks
```

```
[+] WordPress theme in use: proficient
 | Location: https://brainfuck.htb/wp-content/themes/proficient/
 | Last Updated: 2021-10-20T00:00:00.000Z
 | Readme: https://brainfuck.htb/wp-content/themes/proficient/readme.txt
 | [!] The version is out of date, the latest version is 3.0.59
 | Style URL: https://brainfuck.htb/wp-content/themes/proficient/style.css?
ver=4.7.3
 | Style Name: Proficient
 | Description: Proficient is a Multipurpose WordPress theme with lots of
powerful features, instantly giving a prof...
 | Author: Specia
 | Author URI: https://speciatheme.com/
 |
 | Found By: Css Style In Homepage (Passive Detection)
 |
 | Version: 1.0.6 (80% confidence)
 | Found By: Style (Passive Detection)
 |  - https://brainfuck.htb/wp-content/themes/proficient/style.css?ver=4.7.3, Match: 'Version: 1.0.6'

+] wp-support-plus-responsive-ticket-system
 | Location: https://brainfuck.htb/wp-content/plugins/wp-support-plus-responsive-ticket-system/
 | Last Updated: 2019-09-03T07:57:00.000Z
 | [!] The version is out of date, the latest version is 9.1.2
 |
 | Found By: Urls In Homepage (Passive Detection)
 |
 | Version: 7.1.3 (100% confidence)
 | Found By: Readme - Stable Tag (Aggressive Detection)
 |  - https://brainfuck.htb/wp-content/plugins/wp-support-plus-responsive-ticket-system/readme.txt
 | Confirmed By: Readme - ChangeLog Section (Aggressive Detection)
 |  - https://brainfuck.htb/wp-content/plugins/wp-support-plus-responsive-ticket-system/readme.txt
```

Passive scan returns one outdated theme and plugin. Lets ask our best friend google if it has any vulnerabilities present for these versions. There is an exploit for this plugin by which you can login as administrator without needing a password. https://www.exploit-db.com/exploits/41006

Exploit:

Create a html file, copy the POC, change the email address and value to admin and open with your browser and click on submit. Now go to admin panel /wp-admin and you will get redirected to admin dashboard.



Dashboard

Welcome to WordPress!
We've assembled some links to get you started:

Get Started

or, change your theme completely

Next Steps

Write your first blog post
Add an About page
View your site

More Actions

Manage widgets or menus
Turn comments on or off
Learn more about getting started

At a Glance

1 Post
2 Pages
1 Comment
WordPress 4.7.3 running Proficient theme.
Search Engines Discouraged

Quick Draft

Title
What's on your mind?

Activity

Recently Published
Apr 17th 2017, 5:15 pm Dev Update

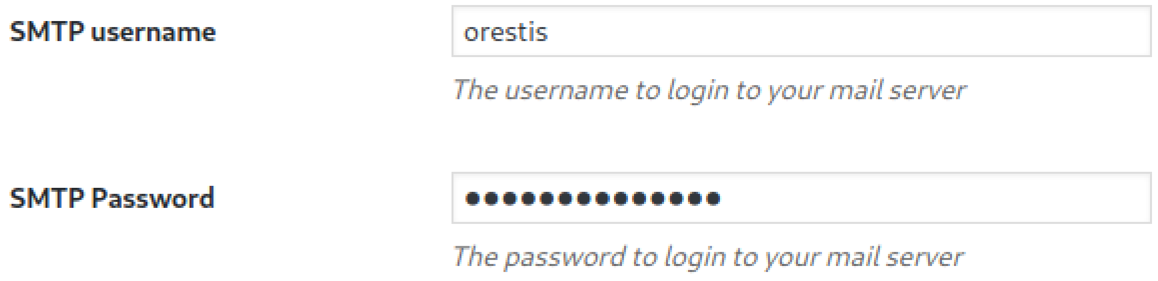
Recent Comments
From A WordPress Commenter on Dev Update
Hi, this is a comment. To get started with moderating, editing, and deleting comments, please visit the

WordPress News

RSS Error: WP HTTP Error: stream_socket_client(): php_network_getaddresses: getaddrinfo failed: Temporary failure in name resolution stream_socket_client(): unable to connect to tcp://wordpress.org:80 (php_network_getaddresses: getaddrinfo failed: Temporary failure in name resolution)

Gaining Initial Foothold:

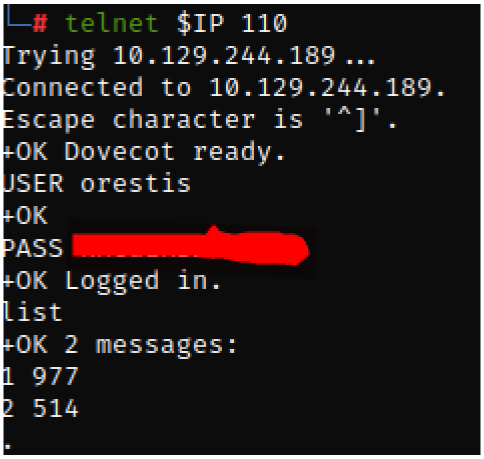
After enumerating this dashboard for 30 mins, I found creds for smtp server in smtp plugin settings.



SMTP username orestis
The username to login to your mail server

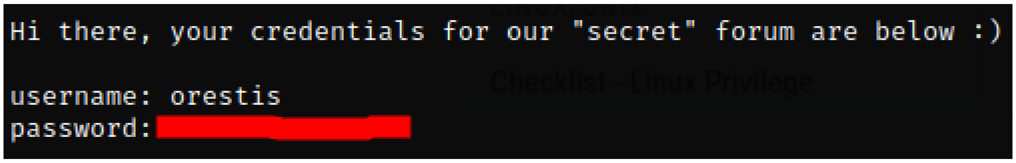
SMTP Password •••••••••••••••
The password to login to your mail server

You can use developer tools to unmask these characters and see the password.
Now we can use these creds to login to pop3 server and see if we have any messages for us. This link https://book.hacktricks.xyz/pentesting/pentesting-pop is a wonderful site where you learn more about pentesting pop3.



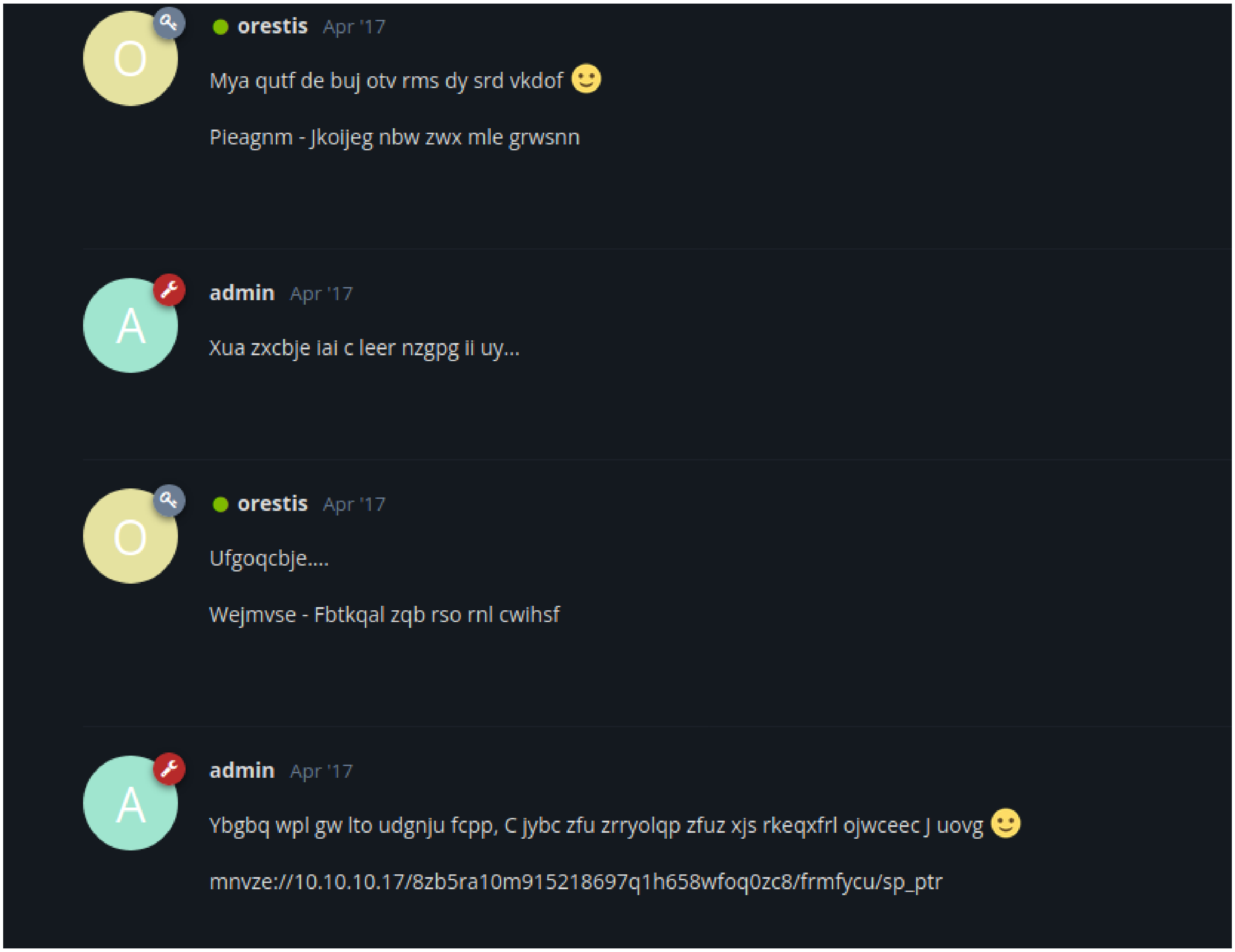
```
└─# telnet $IP 110
Trying 10.129.244.189...
Connected to 10.129.244.189.
Escape character is '^]'.
+OK Dovecot ready.
USER orestis
+OK
PASS [redacted]
+OK Logged in.
list
+OK 2 messages:
1 977
2 514
.
```

Ahah. We got in. We can see we have two messages for us. First message is just a mail for wordpress installation. Second mail is where things get interesting. It contains creds for the super secret forum which we discovered way back in the certificate.



```
Hi there, your credentials for our "secret" forum are below :)

username: orestis
password: [redacted]
```

Now lets go to secret forum and see whats waiting for us.
From what I understand theres a discussion between the user and admin about ssh access. The user orestis cannot ssh into the machine. Admin has sent him the key link but the discussion is all encrypted.



orestis Apr '17

Mya qutf de buj otv rms dy srd vkdof 🙂

Pieagnm - Jkoijeg nbw zwx mle grwsnn

admin Apr '17

Xua zxcbje iai c leer nzgpg ii uy...

orestis Apr '17

Ufgoqcbje....

Wejmvse - Fbtkqal zqb rso rnl cwihsf

admin Apr '17

Ybgbq wpl gw lto udgnju fcpp, C jybc zfu zrryolqp zfuz xjs rkeqxfrl ojwceec J uovg 🙂

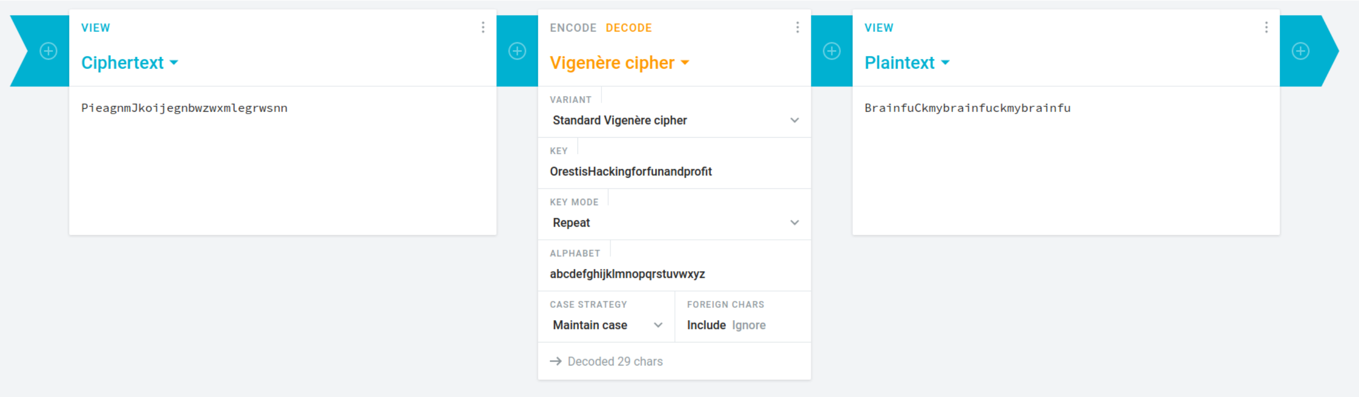
mnvze://10.10.10.17/8zb5ra10m915218697q1h658wfoq0zc8/frmfycu/sp_ptr

There's a great site https://gchq.github.io/CyberChef/ (CyberChef) where you can do trial and error, encode, decode and encrypt and decrypt.
I used cyberchef but couldn't reach anywhere. Well at last, I have to admit, I am not good at cryptography so I went to Ippsec's website for some hints for the decryption part. The hint is Vigenere Cipher. Orestis uses this phrase:

"Orestis - Hacking for fun and profit" everytime after his comment. In encrypted thread after his comment, this same phrase is present but it is encrypted. So now we have ciphertext and plaintext and using these two we will get the decryption key. From one of the writeups I saw this wonderful explanation of Vigenere cipher:
vigenere cipher is the most common substitution cipher that can encode same plaintext string into different ciphertext based on its position in the message

```
    Encode -> PT + Key = CT (when encoding, we just add the key to the plainText to get the cipherText)
    Decode -> PT = CT - Key (when decoding, we just subtract the key from cipherText to get the plainText)
    Decode -> Key = CT - PT (similarly to get the key, we can subtract plainText from cipherText)
```

Using this link https://cryptii.com/pipes/vigenere-cipher we get the key "fuckmybrain"
Remember to remove hyphens and spaces from the ciphertext and plaintext while trying to get the key.



Ciphertext

```
PieagnmJkoijegnbwzwxmlegrwsnn
```

Vigenère cipher

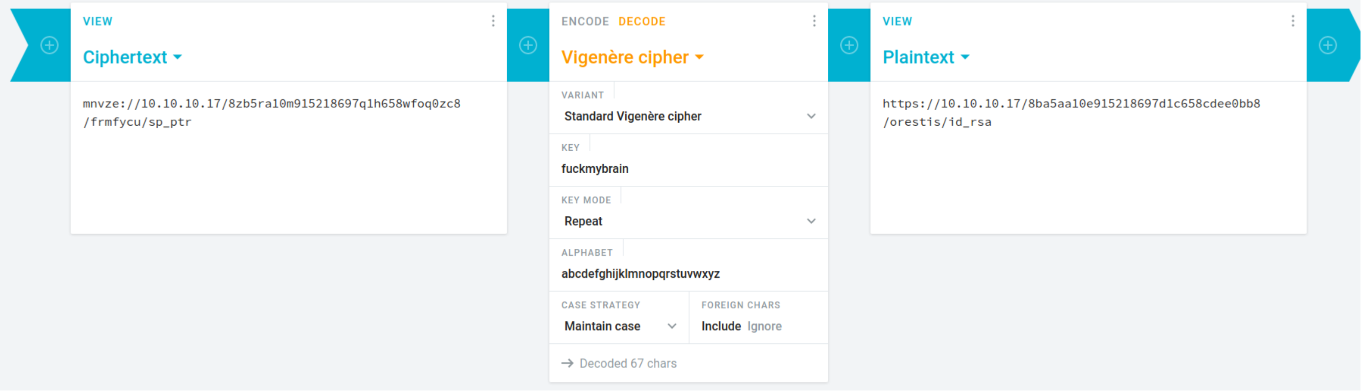
VARIANT: Standard Vigenère cipher
KEY: OrestisHackingforfunandprofit
KEY MODE: Repeat
ALPHABET: abcdefghijklmnopqrstuvwxyz
CASE STRATEGY: Maintain case
FOREIGN CHARS: Include Ignore

→ Decoded 29 chars

Plaintext

```
BrainfuCkmybrainfuckmybrainfu
```

From the thread, we can infer that the admin has sent a link to Orestis. Lets decrypt that and get to the key.



Ciphertext

```
mnvze://10.10.10.17/8zb5ra10m915218697q1h658wfoq0zc8
/frmfycu/sp_ptr
```

Vigenère cipher

VARIANT: Standard Vigenère cipher
KEY: fuckmybrain
KEY MODE: Repeat
ALPHABET: abcdefghijklmnopqrstuvwxyz
CASE STRATEGY: Maintain case
FOREIGN CHARS: Include Ignore

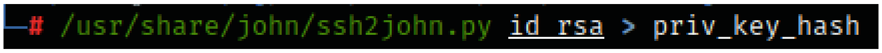
→ Decoded 67 chars

Plaintext

```
https://10.10.10.17/8ba5aa10e915218697d1c658cdee0bb8
/orestis/id_rsa
```

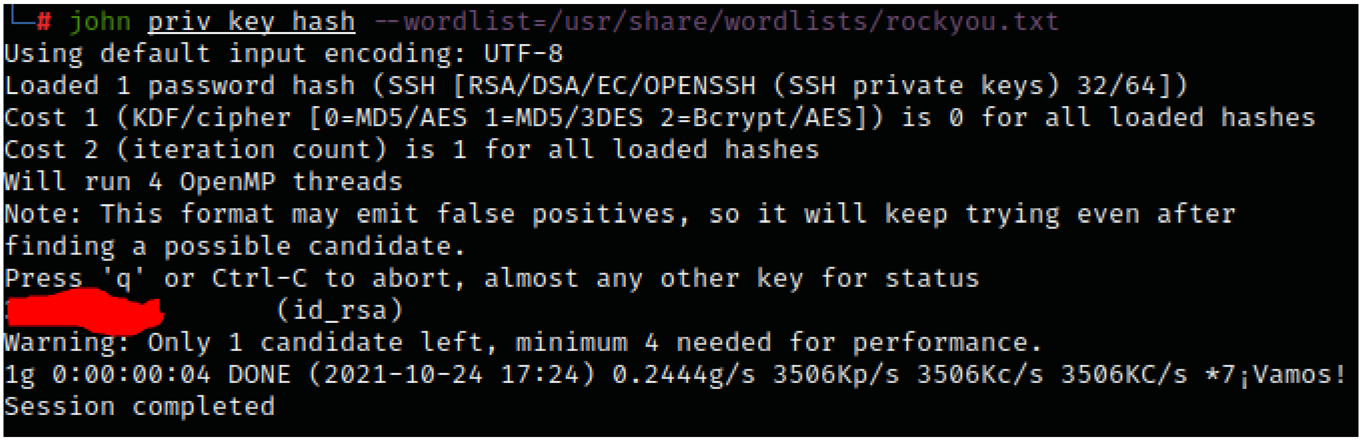
SSH Access as Orestis:

We have the key but to login we also need the passphrase for the key as it is encrypted. Lets call our friend john to do this work for us. First using ssh2john, convert the key to a format which john can understand.



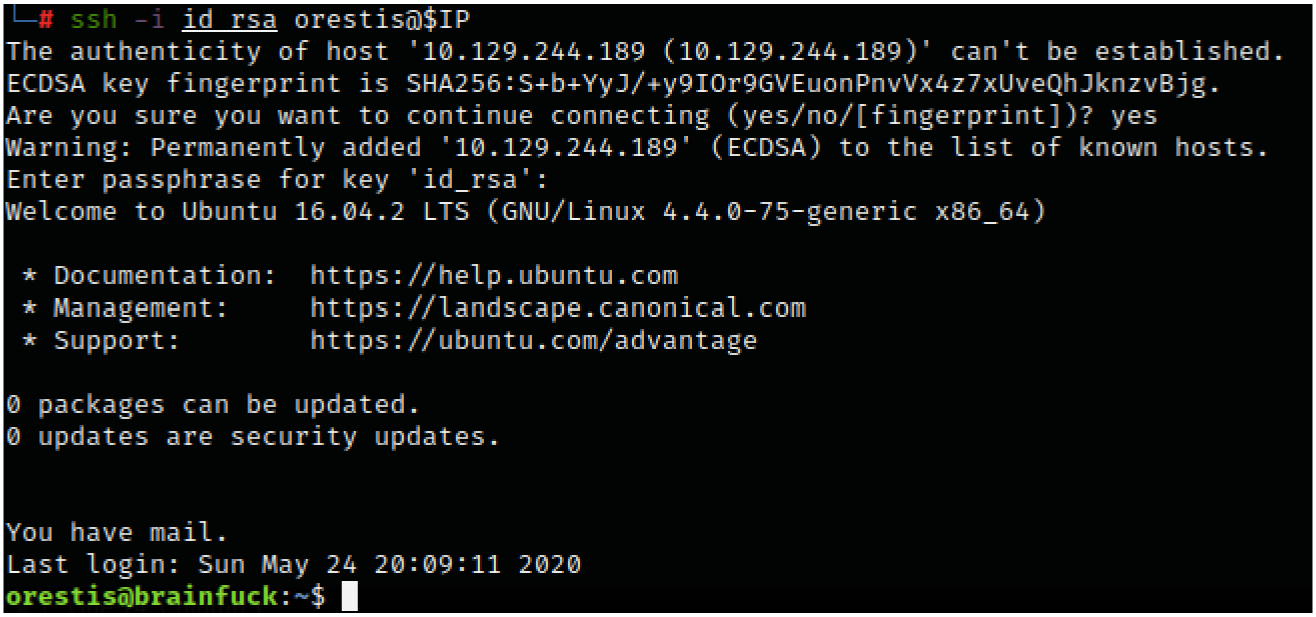
```
└─# /usr/share/john/ssh2john.py id_rsa > priv_key_hash
```

Now, throw this file to john and using the wordlist rockyou, hold tight, you will have the key in no time.



```
└─# john priv_key_hash --wordlist=/usr/share/wordlists/rockyou.txt
Using default input encoding: UTF-8
Loaded 1 password hash (SSH [RSA/DSA/EC/OPENSSH (SSH private keys) 32/64])
Cost 1 (KDF/cipher [0=MD5/AES 1=MD5/3DES 2=Bcrypt/AES]) is 0 for all loaded hashes
Cost 2 (iteration count) is 1 for all loaded hashes
Will run 4 OpenMP threads
Note: This format may emit false positives, so it will keep trying even after
finding a possible candidate.
Press 'q' or Ctrl-C to abort, almost any other key for status
[redacted]        (id_rsa)
Warning: Only 1 candidate left, minimum 4 needed for performance.
1g 0:00:00:04 DONE (2021-10-24 17:24) 0.2444g/s 3506Kp/s 3506Kc/s 3506KC/s *7¡Vamos!
Session completed
```

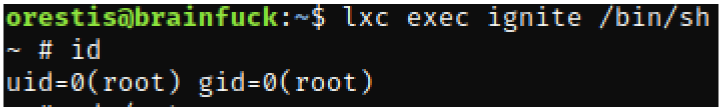
Change the permissions of the key to 600, enter the passphrase and voila you are in:



```
└─# ssh -i id_rsa orestis@$IP
The authenticity of host '10.129.244.189 (10.129.244.189)' can't be established.
ECDSA key fingerprint is SHA256:S+b+YyJ/+y9IOr9GVEuonPnvVx4z7xUveQhJknzvBjg.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.129.244.189' (ECDSA) to the list of known hosts.
Enter passphrase for key 'id_rsa':
Welcome to Ubuntu 16.04.2 LTS (GNU/Linux 4.4.0-75-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

0 packages can be updated.
0 updates are security updates.


You have mail.
Last login: Sun May 24 20:09:11 2020
orestis@brainfuck:~$
```

Privilege Escalation

Now comes the last part. Transfer our favorite linpeas to the machine and let it do the heavylifting for us. At the very top of the output, lxd gets highlighted as out Priv Esc vector. Follow each and every step carefully in this link:
https://www.hackingarticles.in/lxd-privilege-escalation/
Once you have followed all the steps listed, type id and you are root!!!



```
orestis@brainfuck:~$ lxc exec ignite /bin/sh
~ # id
uid=0(root) gid=0(root)
```

Voila!! We have successfully pwned this machine. This machine is rated as insane at hackthebox but for me except the crypto part where I got stuck, rest was just enumeration. Overall, It was really a fun box. Happy Hacking.